GENERAL

1. With the evolving integration of conventional, irregular and cyber capabilities, the contemporary landscape of warfare is undergoing with a substantial transformation. This trend has been generally identified as a hybrid or multi-domain warfare that produces both opportunities and challenges for any military organisations worldwide. In this backdrop, traditional approaches to warfare are no longer sufficient and due to that armed forces need to develop adaptable and innovative strategies to maintain its effectiveness.

2. Concerning the Sri Lanka military, Sri Lanka Army as one of the most recognized armies in the world with its notable history of successful campaign against terrorism, these developments demand a paradigm shift of all aspects. Similar to any militaries, Sri Lanka Army must now face with non-traditional security challenges in various forms including cyber threats, information warfare and irregular tactics employed by state and non-state actors. These complexities demand a unified approach to integrate diverse capabilities, fostering interoperability between other services and enhancing operational readiness.

3. This study aims to research into the challenges connected with this evolving nature of warfare, particularly as they relate to the Sri Lanka Army's unique operational context. It will analyse the implications of integrating conventional, irregular and cyber warfare capabilities and offer evidence-based recommendations to ensure the Army's continued effectiveness in safeguarding national security. By addressing these issues, the research seeks to contribute to the strategic development of the Sri Lanka Army, focusing contemporary and future security demands with resilience and adaptability.

BACKGROUND OF THE RESEARCH

4. After the World War I mainly during Cold War era, the rapid advancements in technology have transformed traditional warfare to the rise of hybrid challenges.

Although the conventional military forces remain crucial in safeguarding country's national security, irregular tactics and cyber warfare have gained dominance, demanding a comprehensive and integrated approach. Hence, to face those hybrid challenges, the term "hybrid warfare" came on to the forum. Hybrid warfare is a combination of conventional military force, irregular tactics cyber warfare, disinformation, economic sanctions and other non-traditional means used simultaneously to exploit an adversary' vulnerabilities.

5. Sri Lanka's geo-strategical location and past experiences with its internal conflict make it an ideal case study for examining the necessity and feasibility of integrating these warfare domains. However, this transition involves addressing conceptual, moral and physical components of fighting power. In the fifteen years since the end of war against LTTE, Sri Lanka has faced numerous security compulsions shaped by both internal and external dynamics. Domestically, with the concept of "5R" the government prioritised rehabilitation and reintegration of former LTTE combatants to prevent any rebirth of separatism. Programmes focused on skills development, employment and psychological support aimed to reintegrate ex-combatants to the society. Simultaneously, rebuilding war-torn areas in the Northern and Eastern Provinces became a critical focus. But, addressing ethnic tensions and grievances remained a persistent challenge whereas reconciliation efforts faced difficulties. Post-war Sri Lanka also had to contend with new security threats, such as organized crime, drug trafficking and the rise of extremist groups, as evidenced by the 2019 Easter Sunday terror attacks, which highlighted the weaknesses of national intelligence and counter-terrorism mechanisms.

6. Externally, Sri Lanka's strategic location has made it a focal point of global and regional power competition. The country has had to navigate the growing rivalry between India and China, both have entrusted economic and geopolitical interests in the region. Chinese investments in Sri Lanka's infrastructure under the Belt and Road Initiative have provided significant economic benefits but also raised concerns about sovereignty and debt dependency. This has challenged relations with India which remains suspicious of China's growing presence in its neighborhood. Balancing relations with these two major powers as well as maintaining strong partnerships with the United States, Russia, Japan and other allies has been crucial for Sri Lanka to

preserve its strategic autonomy while avoiding entanglement in broader geopolitical tensions.

7. Sri Lanka's maritime security has also been a critical concern since its proximity to key maritime routes in the Indian Ocean. Challenges such as piracy, illegal fishing, human trafficking and maritime smuggling have required significant investment in naval and coast guard capabilities. Moreover, the country supposed to work closely with regional and global allies to ensure the security of its Exclusive Economic Zone and combat transnational threats.

8. Beyond traditional security threats, climate change and environmental challenges have also emerged as significant non-traditional threats. Rising sea level, unpredictable weather patterns and coastal corrosion threaten Sri Lanka's agriculture and fisheries-dependent communities.

9. Sri Lanka's security compulsions are further complicated by its economic vulnerabilities and international pressure. Post-war reconstruction, corruptions and economic mismanagement have left the country's economy indebted to China and international financial institutions. The economic crisis in year 2022 highlighted the problem of the nation's financial system. Moreover, continuation of the Tamil diaspora's activities made the government under constant examination by Western nations and organisations like the UNHRC. Those internal and external threats highlight the multifaceted post-war environment Sri Lanka faces which require a balanced approach to ensure national security in a rapidly changing regional and global context.

RESEARCH OBJECTIVES

10. Research objectives of this study can be considered as follows:

a. To analyse the current state of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.

b. To identify challenges in achieving integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.

c. To evaluate strategies adopted by international militaries in hybrid warfare integration.

d. To propose recommendations for the effective integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.

PROBLEM STATEMENT

11. Sri Lanka Army presently faces several challenges in effectively integrating conventional, irregular and cyber warfare capabilities due to organisational structures, technological and financial limitations and doctrinal gaps. This integration is necessary for addressing evolving security threats in the contemporary battlefield environment.

CORE ARGUMENT

12. The integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army is necessary for enhancing its operational readiness and adaptability to contemporary security dynamics. Addressing organisational, doctrinal, financial and technological challenges is vital in implementing a cohesive and effective hybrid warfare capabilities.

RESEARCH QUESTIONS

13. The research questions which derived from the study are as follows:

a. What are the current gaps in the integration of hybrid warfare capabilities within the Sri Lanka Army?

b. How do organisational structures and doctrine support or hinder capability integration?

c. What lessons can be derived from international military forces' experiences in warfare capability integration?

d. What specific reforms are required to achieve effective integration of these capabilities?

SIGNIFICANCE OF THE STUDY

14. This study aims to addresses a critical gap in modernizing the military with specific focus to the Sri Lanka Army context. Those findings will:

a. Contribute to the implementation of integrated warfare doctrine for the Sri Lanka Army.

b. Inform policy-makers regarding necessities of military modernization.

c. Enhance the Sri Lanka Army's ability to respond to evolving contemporary security challenges.

d. Afford valuable insights for other militaries who are facing similar integration challenges.

SCOPE AND LIMITATIONS

15. The research focuses on the Sri Lanka Army's efforts in integrating conventional, irregular and cyber warfare capabilities by making comparisons with

other nations' militaries to identify relevant lessons. During the process, the researcher may undergo restraints in accessing classified information and limitations in the availability of comprehensive details on cyber warfare capabilities.

STRUCTURE OF THE THESIS

16. This study consists of six chapters as follows:

a. **Chapter One.** Provides an overview of the research topic, including the problem statement, objectives, significance, scope, and structure.

b. **Chapter Two.** Reviews literature on hybrid warfare, military integration, and case studies from other nations.

c. **Chapter Three.** Details the research methodology, data collection methods, and analytical techniques.

d. **Chapter Four.** Presents findings based on qualitative data and comparative studies.

e. **Chapter Five.** Discusses key findings and their implications for the SLA.

f. **Chapter Six.** Concludes the study and offers recommendations for hybrid warfare capability integration.

17. This structured approach ensures a comprehensive analysis of hybrid warfare integration within the SLA, providing actionable recommendations for military modernization.

LITERATURE REVIEW

INTRODUCTION

1. The contemporary security environment is characterized by increasing complexity, demanding an exit from traditional tactics and isolated approaches to warfare. Contemporary conflicts are no longer can be categorized specifically, as state and non-state actors employ a diverse range of methods to achieve their goals. Hence, the integration of conventional, irregular and cyber warfare capabilities has emerged as a crucial adaptation for present-day militaries seeking to address this multifaceted threat landscape successfully. This integration allows identification of synergistic effects, leveraging the unique strengths of each domain to present adversaries with complex and overlapping challenges (Hoffman, 2007).

2. This literature review will explore the existing knowledge on these distinct forms of warfare, the theoretical and practical aspects of their integration, and the specific context of the Sri Lanka Army, which has a rich history of engaging in both conventional and irregular conflicts. By examining the challenges and potential benefits of this integration, this review aims to provide a foundation for understanding the evolving nature of warfare and the adaptations necessary for the Sri Lanka Army to maintain its effectiveness in the 21st century.

THEORETICAL FOUNDATIONS OF WARFARE

3. The study of warfare has been considered in both traditional and modern theoretical perspectives. Carl von Clausewitz (1832)'s "On War" suggests that war is a continuation of politics by other means, emphasizing the importance of strategy, statecraft and the role of the military as an instrument of state policy. Clausewitz's

"trinity" of people, army and government still foundational in understanding the general nature of war.

4. In contrast, Sun Tzu's "The Art of War" emphasize deception, strategic maneuver and indirect engagement are increasingly relevant in the age of irregular and cyber warfare. These foundational theories have evolved to accommodate contemporary security environments, giving rise to hybrid and multi-domain warfare concepts.

5. The theory of "Hybrid Warfare" as articulated by (Hoffman, 2007) bridges the gap between conventional and unconventional operations, combining elements from multiple domains into a singular, adaptive approach. Luddy, (2005) highlights, the emergence of network-centric warfare and complex adaptive systems theory further supports the concept of modern conflict environments require flexible, integrative frameworks that control various military capabilities.

DEFINING CONVENTIONAL WARFARE

6. Conventional warfare, at its core, involves a direct military confrontation between two or more states utilizing conventional weapons and battlefield tactics in open engagement (Razma, 2019). The primary aim in such conflicts is to weaken or destroy the opponent's military forces, thereby negating their ability to wage conventional war and ultimately compelling defeat (Duyvesteyn, 2005). This form of warfare is typically distinguished by the exclusion of nuclear, biological, chemical, or radiological weapons (Saunders-Price, 2020). As highlighted by the US Department of Defence, (2007) conventional military operations often focus on an adversary's armed forces with the objective of influencing the adversary's government or policies. This underscores the inherent political dimension of conventional warfare, where military actions are ultimately aimed at achieving political objectives.

7. Even though most wars have been conducted through conventional means the continuation of large-scale conventional warfare in the 21st century is debatable (Cassese, 2023). Scholars such as Payne, (2017) and Gray, (2011) argue that opponents recognizing the conventional superiority of forces like the United States military, are

tend to pursue indirect and some unconventional approaches to achieve their strategic gains.

8. The rise of "hybrid threats" which blend conventional and irregular methods, further challenges the traditional understanding of warfare (Naseeb, 2024). Despite these challenges, conventional warfare remains crucial for power. However, as seen in recent conflicts, inferior force may find success by avoiding direct conventional engagements with a superior enemy that highlights the limitations of relying solely on conventional strength (Hoffman, 2014). This suggests that a balanced approach, integrating conventional capabilities with other forms of warfare is essential for modern militaries.

IRREGULAR WARFARE IN THEORY AND PRACTICE

9. Irregular warfare involves the use of unconventional tactics by state and non-state actors to undermine a superior adversary. This form of warfare includes guerrilla warfare, insurgency, terrorism and sabotage. Sitaraman, (2009) and (Shamieh, 2021) highlight the role of local population support, information operations and decentralization of force as the success of irregular strategies.

a. **Guerrilla warfare.** Guerrilla warfare, one of the most well-known forms, involves small groups of irregular forces utilizing ambushes, sabotage, raids and hit-and-run tactics against a larger and more conventional adversary (Joes, 1996).

b. **Insurgency.** An insurgency is a movement within a country dedicated to overthrowing the government. An insurgency is a rebellion. Insurgencies are movements to overthrow governments (O'Neill, 1980).

c. **Counterinsurgency.** Counterinsurgency represents a comprehensive effort, involving both civilian and military components, designed to simultaneously defeat and contain an insurgency while addressing its underlying root causes (Kilcullen, 2010).

d. **Terrorism.** Terrorism is the calculated use of violence or the threat of violence to create a climate of fear and achieve political or ideological goals. It is often characterized by the targeting of civilians to instill fear and coerce a government or population into action (Saunders-Price, 2020).

10. Irregular warfare is not a new phenomenon. Throughout history, it has been a persistent feature of conflict, with estimates suggesting that approximately 80% of warfare since the Napoleonic era has been irregular in nature (Deckard and Shapiro, 2019). In the context of great power competition, irregular warfare remains highly significant, as states often employ indirect methods to advance their interests and undermine their rivals without resorting to direct military confrontation (Hoffman, 2006). The historical evolution of irregular warfare demonstrates its adaptability, from ancient asymmetrical confrontations to the complex dynamics of modern insurgencies and counter-insurgencies, including the rise of terrorism as a weapon (Tripodi, 2025).

11. Benyamin et al., (2023), discusses the relationship between irregular and conventional warfare is not always clear-cut. Adversaries frequently employ methods from both categories, adapting their approach to the specific context of the conflict. In some instances, irregular warfare can even be considered a subset of conventional warfare, particularly when examining counter-revolutionary efforts.

12. Irregular warfare challenges the conventional model by avoiding symmetric confrontations. During the Sri Lankan civil war, the Liberation Tigers of Tamil Eelam (LTTE) utilized irregular tactics including suicide bombings, ambushes, air power and maritime insurgency. These experiences illustrate the need for the Sri Lanka Army to retain and further develop irregular warfare competencies alongside conventional capabilities (Hashim, 2013).

13. Mumford and Carlucci, (2023) highlights as, the lines between these forms of warfare have become increasingly blurred in modern conflicts, giving rise to the concept of “hybrid warfare” where states and non-state actors integrate conventional and irregular tactics to achieve their objectives.

THE DOMAIN OF CYBER WARFARE

14. Cyber warfare represents a fundamental shift in the character of warfare. Unlike other warfare, cyber conflict is mostly non-kinetic, transnational and anonymous in nature. Taillat, (2024) defines cyber war as the use of digital attacks to cause physical destruction, disruption, or strategic dislocation. Nye, (2018) and van Haaster, (2016) describes cyber power as the ability to use cyberspace to influence others' behavior or outcomes. It involves the use of digital techniques, technologies, and tactics to conduct aggressive and strategic actions against adversaries, encompassing cyberattacks, espionage, and information warfare (Bardin, 2025).

15. The capabilities within cyber warfare are diverse, including espionage aimed at stealing sensitive information, sabotage intended to disrupt or damage systems, denial-of-service attacks that prevent legitimate users from accessing online services, propaganda attacks designed to manipulate public opinion and economic disruption targeting financial institutions and critical economic infrastructure (Lehto, 2022). These capabilities highlight the significant impact that digital operations can have on modern conflicts and global security.

16. The strategic implications of cyber warfare for national security and military operations are far-reaching. Successful cyberattacks can disrupt essential services, cripple economies and could damage a nation's reputation. Azad and Haider, (2020) stresses, attacks targeting military networks can compromise classified information and communication systems, thereby endangering military operations. Cyber espionage undermines national security by facilitating the theft of sensitive data, including government secrets and military plans (Banks, 2016).

17. Despite global recognition of cyber as a fifth domain of warfare, Sri Lanka's cyber defence capacity remains developing. The absence of a dedicated military cyber command, insufficient legislative frameworks and lack of inter-agency coordination are critical impediments to operational readiness (Bentototahewa, 2021).

HYBRID WARFARE AS MERGING OF DOMAINS

18. Hybrid warfare, as defined by Hoffman, (2007) involves the simultaneous and adaptive use of conventional weapons, irregular tactics, cyber tools and psychological operations to achieve strategic goals. It is predicated on ambiguity, rapid tempo and multidimensional threat trajectories.

19. Mumford and Carlucci, (2023) outlines the Russian perspective on hybrid operations, which blend non-military measures with kinetic force. Mohee, (2022) and the Hybrid Threat Centre of Europe Union identify the combination of cyber, economic and political warfare as key elements. The hybrid warfare model necessitates flexible doctrines, interoperable forces and intelligence-driven command structures.

20. Theoretical frameworks such as Boyd's OODA loop (Observe, Orient, Decide, Act) theory which indicated in figure 2.1 offer insights into decision-making and adaptability in hybrid conflicts. These models underscore the importance of speed, decentralization and structures thinking in modern military operations (Johnson, 2023).

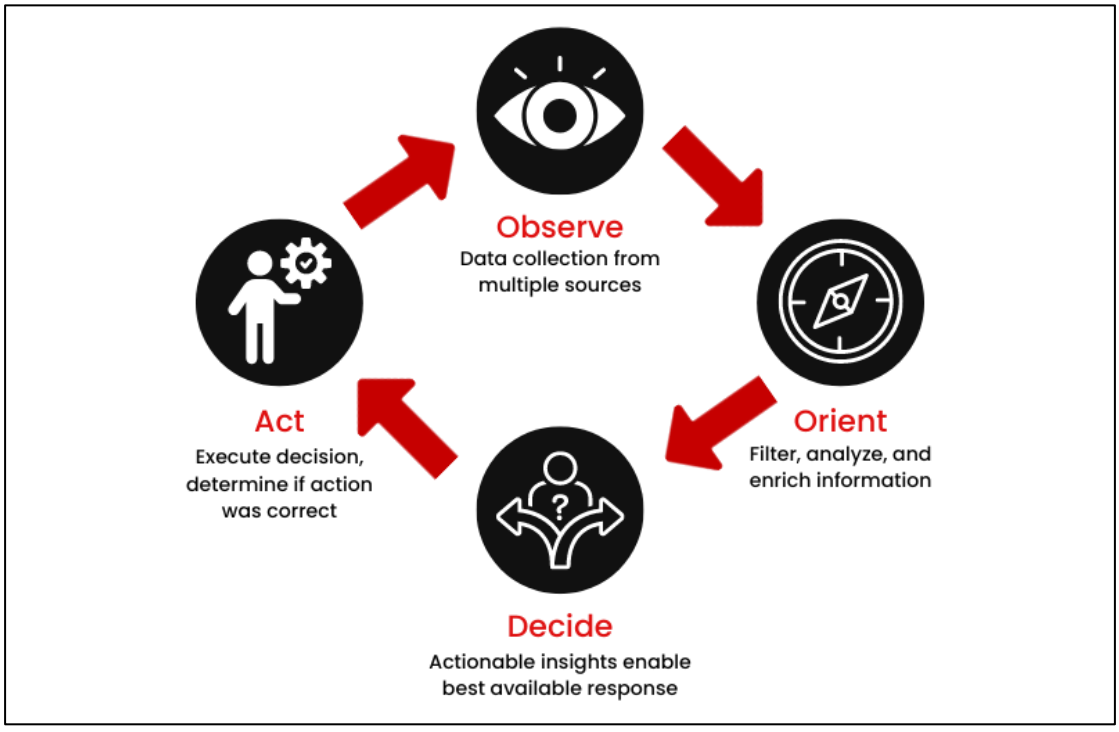

Figure 2.1: Boyd's OODA Loop

Source: Johnson, (2023)

INTEGRATION OF CONVENTIONAL, IRREGULAR AND CYBER WARFARE

21. The increasing complexity of the modern security environment necessitates a move beyond viewing conventional, irregular and cyber warfare as distinct and mutually exclusive categories (Razma, 2019). A holistic approach that strategically merges these capabilities is essential for modern militaries to effectively address the diverse threats they face. As Hoffman, (2007) elaborates, this integration aims to create synergistic effects, where the combined impact of these capabilities exceeds the sum of their individual parts.

22. The concept of hybrid warfare provides a theoretical framework for understanding this integration. It describes the simultaneous use of multiple types of warfare by flexible and sophisticated adversaries (Otaiku, 2018). This often involves a blend of conventional and irregular methods, incorporating cyber warfare, information operations, and economic pressure, all coordinated to achieve strategic objectives without resorting to overt, large-scale conventional conflict. Azad et al., (2023) argues, Hybrid warfare frequently operates in the "gray zone" a space below the threshold of traditional armed conflict, where the lines between war and peace are blurred.

23. Naseeb, (2024) and Duyvesteyn, (2005) highlights, the potential benefits of effectively integrating conventional, irregular and cyber warfare capabilities are significant. It can lead to enhanced deterrence by presenting a more complex and unpredictable threat to potential adversaries. Operational effectiveness is increased through the synergy of cross-domain effects, allowing for more comprehensive and impactful operations. Integrated capabilities improve the ability to counter diverse and adaptive adversaries who may employ a mix of conventional and unconventional tactics. Furthermore, Giegerich, (2016) believes, it provides greater flexibility and

adaptability in responding to a wide range of conflict scenarios, from traditional state-on-state warfare to asymmetric engagements and cyberattacks. A comparison of conventional, irregular and cyber warfare aspects has been developed and indicated under Table 2.1.

Table 2.1: Comparison of Conventional, Irregular, and Cyber Warfare

Ser	Characteristic	Conventional Warfare	Irregular Warfare	Cyber Warfare
(a)	(b)	(c)	(d)	(e)
1.	Primary Actors	States or coalitions of states	State and non-state actors	Nation-states, terrorist groups, cybercriminals, hacktivists, individuals
2.	Typical Tactics	Maneuver, massed firepower, open confrontation	Ambushes, sabotage, raids, guerrilla tactics, terrorism, subversion	Espionage, sabotage, denial-of-service, propaganda, economic disruption
3.	Objectives	Weaken/destroy opponent's military, gain territory	Secure/maintain legitimacy, erode adversary's power and will, influence populations	Disrupt systems, steal data, influence public opinion, gain strategic advantage
4.	Weapons Used	Conventional weapons (tanks, artillery, aircraft)	Improvised weapons, small arms, asymmetric means	Digital tools, malware, networks, information
5.	Environment of Op.	Open battlefields, defined front lines	Among civilian populations, denied areas, urban environments	Cyberspace, interconnected networks

Source: Developed by the researcher (2025).

INTERNATIONAL APPROACHES TO WARFARE INTEGRATION

24. Contemporary militaries worldwide are adopting with the approach of integration of warfare for their operational success. Several case studies with literature discussed below.

a. **The United States of America.** The US military has been at the forefront of integration efforts, exemplified by its Joint All-Domain Command and Control (JADC2) framework and the structure of unified combatant commands. A key component is United States Cyber Command (USCYBERCOM), which works in continually with regular and special operations forces to improve battlefield understanding and the ability to deploy forces effectively (US Department of Defence, 2007)

b. **Russia.** Russia has demonstrated effective integration in its hybrid warfare campaigns, particularly noted in Ukraine and Georgia. These operations synchronized cyber warfare, unconventional militias, and standard military formations. Muradov, (2022) briefs, this strategy aligns with the Gerasimov Doctrine by emphasizing dominance in the information space, influencing adversary decision-making and maintaining strategic uncertainty.

c. **India.** Facing threats on several borders, India is actively pursuing military integration. Subramaniam, (2023) highlights, their key initiatives include creating the Defence Cyber Agency, a dedicated Special Forces Division and developing Integrated Battle Groups (IBGs). Indian military modernization emphasizes enhanced cooperation between the army, navy and air force (tri-service), building cyber resilience and strengthening asymmetric warfare capabilities (Hariz, 2019).

d. **Bangladesh.** Bangladesh is modernizing its military through the "Forces Goal 2030" plan, aiming to create a well-equipped and integrated Army, Navy and Air Force capable of handling modern threats (Akter and Rafah, 2024). Coordinated by the Armed Forces Division (AFD), they are

aiming to counter misinformation and leverage intelligence from sources like social media, while integrating advanced surveillance (ISR) and Artificial Intelligence (AI).

EVOLUTION OF SRI LANKA ARMY

25. The Sri Lanka Army, established in 1949 as the Ceylon Army and renamed in 1972, is the oldest and largest component of the Sri Lanka Armed Forces. Throughout the history, due to dynamics of country's security landscape the nature of war-fighting and tactics have been evolved differently. Hence this evolution from the inception up to the end of civil war has been tabulated as indicated under Table 2.2 below.

Table 2.3: Evolution of Sri Lanka Army Tactics and Equipment

Ser	Phase	Period	Dominant Tactics	Key Equipment
(a)	(b)	(c)	(d)	(e)
1.	Pre-Eelam War	1949-1983	Internal security, assisting police, ceremonial duties	Primarily small arms inherited from British colonial forces
2.	Eelam War-One	1983-1990	Counter-insurgency, conventional formations against guerrilla tactics	Infantry weapons, limited armor and artillery
3.	Eelam War-Two	1990-1995	Positional defence, seeking to clear rebel-dominated areas, LTTE employing terror acts and unconventional warfare	Conventional infantry weapons, LTTE using IEDs, small arms, suicide attacks
4.	Eelam War-Three	1995-2006	Conventional warfare in north and east, LTTE attacks including suicide bombings	Increased use of armor, artillery, air support by SLAF. LTTE with artillery, naval and air capabilities, suicide cadres
5.	Eelam War-	2006-2009	Small, independent teams (SIOTs), deep	Improved small arms, precision fire guidance,

	Four		penetration, combined arms, joint operations, Information operations	enhanced naval capabilities (Arrow boats), Blue-water attacks, air reconnaissance and Laser Guided Bombing, LTTE initially with heavy weaponry but gradually decimated

Source: Developed by the researcher (2025).

26. By April 2025, the Sri Lanka Army has approximately 125000 personnel. The majority of troops are deployed for domestic defence and internal security duties across the island. Looking towards the future, as Fernando, (2024) highlights the Sri Lanka Army is undergoing a transformation with the aim of becoming a leaner, more effective and technologically advanced force by the year. This includes a focus on modernization and the integration of new technologies to enhance its capabilities across the spectrum of potential threats.

SPECIFIC CHALLENGES FOR THE SRI LANKA ARMY IN CAPABILITY INTEGRATION

27. Integrating conventional, irregular and cyber warfare capabilities presents a unique set of challenges for the Sri Lanka Army, restricting from technological limitations, doctrinal aspects, historical experiences and external influences (Pathirana, 2024). Overcoming these organizational silos will require fostering a culture of inter-branch cooperation and establishing robust mechanisms for joint planning and execution.

28. **Technological Challenges.** Technological limitations, particularly in the rapidly evolving domain of cyber warfare, pose another significant challenge. While the Sri Lanka Army has plans for technological advancement and has recognized the importance of cyber capabilities resource and financial constraints may hinder the acquisition and implementation of cutting-edge cyber warfare technologies and the development of the necessary infrastructure and skilled personnel (Manangoda, 2022).

29. **<u>Financial Challenges</u>.** While the government has increased the defence budget in recent years, a substantial portion is allocated to recurrent expenditure like salaries, leaving relatively little for capital expenditure necessary for modernization (Sri Lanka's Defence Expenditure from 1983 to 2024 is indicated at figure 2.2) This constraints forces the army to prioritize maintaining its current capabilities over acquiring advanced systems, hindering its ability to adapt to evolving security threats and adopt modern military strategies (Bulathgama, 2022) .

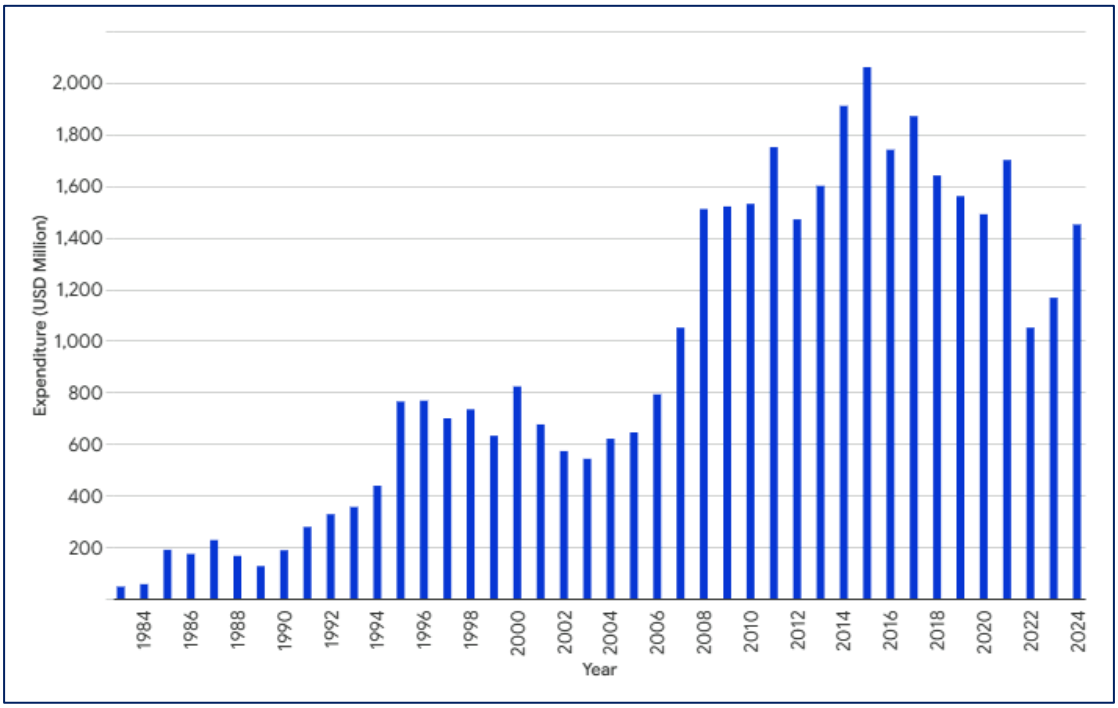

Figure 2.2: Sri Lanka Defence Expenditure (1983 to 2024)

Source: Developed by the author referring Central Bank Reports (2025).

30. **<u>Doctrinal Challenges</u>.** The Sri Lanka Army's military doctrine, although evolving with the adoption of a "Capstone Doctrine" may still need further adaptation to fully address the complexities of integrating cyber capabilities with traditional conventional and irregular warfare methods (Pathirana, 2024). Developing comprehensive training programs that equip personnel with the necessary skills and knowledge to operate effectively across all three domains will be crucial. This includes not only technical training but also fostering a mindset that embraces new approaches to warfare and encourages innovation.

31. **Historical Experiences.** The Army's extensive experience in both conventional and irregular warfare during the civil war provides a valuable foundation for integration (Velch, 2013). Lessons learned from adapting to the LTTE's irregular tactics can inform the approach to integrating cyber capabilities, which, while novel, shares characteristics of asymmetry and the need for adaptability. However, as Bulathgama, (2022) argues cyber warfare also presents unique challenges that require new strategies and doctrines beyond those developed for traditional conflicts.

32. **External Impact.** External influences and partnerships play a role in shaping the Sri Lanka Army's integration efforts. Defence cooperation with regional and global powers can provide access to technology, training and expertise, potentially accelerating the integration process (Joseph, 2019). However, geopolitical considerations and the influence of foreign military doctrines may also present constraints or necessitate careful navigation to align integration efforts with Sri Lanka's specific strategic needs and its commitment to a non-aligned foreign policy.

SRI LANKAN DEFENCE POLICY AND STRATEGIC OUTLOOK

33. Sri Lanka's defence policy, primarily driven by the Ministry of Defence, historically focused on internal security and counter-insurgency. The current strategic outlook emphasizes developing a smaller, technologically advanced and more effective military force through strength re-structuring and equipment modernization across all branches (Fernando, 2024).

34. The Sri Lanka Army has codified its operational principles in a "Capstone Doctrine" that guides training and education. As Pathirana et al., (2023) highlights, institutions like the Sri Lanka Military Academy (SLMA) and the Army Training School (ATS) provide comprehensive military skills and knowledge. Senior officers receive strategic training at the National Defence College (NDC). With Sri Lanka Navy Maritime Doctrine and strategic plan known as "NAVSTRAT-2030" and Air Force doctrinal aspects also indicates their strategic plans (Dhammika, 2024).

35. Recognizing the growing importance of cyber warfare, the Sri Lanka Army has established a Cyber Security Cell under the Directorate of Information Technologies. Dhammika, (2024) highlights, current efforts focus on developing defensive cyber capabilities using AI technologies to secure military networks and protect against cyber threats. The Army collaborates with organizations like SLCERT to enhance cybersecurity skills (Senaratne, 2017).

GAPS OF THE LITERATURE

36. This review of available literature reveals significant gaps in the context of Sri Lanka. Most academic and policy discussions focus on conventional military operations or generic cyber threats. Only a few studies examine the institutional, doctrinal and strategic aspects of hybrid warfare integration within the Sri Lanka Army. There is also a scarcity of interdisciplinary research linking defence studies, cybersecurity and strategic management.

CONCLUSION

37. This literature review has explored the distinct characteristics and evolving relevance of conventional, irregular, and cyber warfare. It has highlighted the theoretical imperative for their integration through concepts like hybrid warfare and multi-domain operations, emphasizing the potential for enhanced deterrence and operational effectiveness. The Sri Lanka Army stands at a crucial juncture in adapting to the complexities of modern warfare. The current focus on technological advancement and the promising development of cyber capabilities indicates a strategic direction towards embracing a more integrated approach.

38. However, the effective integration of these diverse warfare capabilities presents

significant challenges related to organizational structure, technological acquisition, doctrinal adaptation, and leveraging historical lessons. While Sri Lankan defence policy demonstrates an awareness of the need for modernization and cyber security, a more explicit and detailed framework for the integrated employment of conventional, irregular and cyber capabilities will be essential for the Sri Lanka Army to effectively address contemporary security challenges and future threats in an increasingly complex and interconnected world.

LIST OF REFERENCES

Akter, S., Rafah, J., 2024. Bangladesh's Role in a Free and Open Indo-Pacific: A Proposed Strategy. https://doi.org/10.31219/osf.io/4sjb8

Azad, T.M., Haider, M.W., 2020. Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan.

Azad, T.M., Haider, M.W., Sadiq, M., 2023. UNDERSTANDING GRAY ZONE WARFARE FROM MULTIPLE PERSPECTIVES. World Aff. 186, 81–104. https://doi.org/10.1177/00438200221141101

Banks, W.C., 2016. Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. Emory Law J. 66, 513.

Bardin, J.S., 2025. Chapter 87 - Cyber Warfare, in: Vacca, J.R. (Ed.), Computer and Information Security Handbook (Fourth Edition). Morgan Kaufmann, pp. 1345–1380. https://doi.org/10.1016/B978-0-443-13223-0.00087-4

Bentototahewa, V., 2021. A Framework for Acceptance and Implementation of Global Data Privacy and Security Policies by States (A Case Study of Sri Lanka and United Kingdom) (thesis). Cardiff Metropolitan University. https://doi.org/10.25401/cardiffmet.19169306.v1

Benyamin, J., Mualim, M., Duarte, E.P., 2023. Force development against irregular and hybrid warfare in Indonesia. Def. Secur. Stud. 4, 46–51. https://doi.org/10.37868/dss.v4.id234

Bulathgama, T., 2022. Cyber Terrorism an Emerging Threat to Sri Lanka's National Security. Inst. Natl. Secur. Stud. - Natl. Secur. Pap. III, 32.

Cassese, A., 2023. Means of Warfare: The Traditional and the New Law. J. Int. Crim. Justice 21, 1155–1191. https://doi.org/10.1093/jicj/mqad054

Deckard, S., Shapiro, S., 2019. World-Culture and the Neoliberal World-System: An Introduction, in: Deckard, S., Shapiro, S. (Eds.), World Literature, Neoliberalism, and the Culture of Discontent. Springer International Publishing, Cham, pp. 1–48. https://doi.org/10.1007/978-3-030-05441-0_1

Dhammika, K., 2024. THE DOUBLE-EDGED SWORD: ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY IN SRI LANKA. Def. Secur. J. 9, 1–8.

Duyvesteyn, I., 2005. The Concept of Conventional War and Armed Conflict in Collapsed States, in: Rethinking the Nature of War. Routledge.

Fernando, A., 2024. Army will be a leaner, more capable force by 2030: Lt. Gen. Vikum Liyanage [WWW Document]. Latest News Sphere Morning. URL https://themorning.lk//articles/3YHxe3eimwvKjWASWTdo (accessed 4.30.25).

Giegerich, B., 2016. Hybrid Warfare and the Changing Character of Conflict. Connect. Q. J. 15, 65–72. https://doi.org/10.11610/Connections.15.2.05

Gray, C.S., 2011. Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century. Lulu.com.

Hariz, P.M., 2019. Transformation of the Indian Army in the New World Order. CLAWS J. 12, 44–65.

Hashim, A., 2013. When Counterinsurgency Wins: Sri Lanka's Defeat of the Tamil Tigers. University of Pennsylvania Press.

Hoffman, F.G., 2014. Hybrid warfare and challenges, in: Strategic Studies. Routledge.

Hoffman, F.G., 2007. Conflict in the 21st Century: Potom. Inst. Policy Stud.

Hoffman, F.G., 2006. Complex Irregular Warfare: The Next Revolution in Military

Affairs. Orbis 50, 395–411. https://doi.org/10.1016/j.orbis.2006.04.002

Joes, A.J., 1996. Guerrilla Warfare 1–320.

Johnson, J., 2023. Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age. Def. Stud. 23, 43–67. https://doi.org/10.1080/14702436.2022.2102486

Joseph, R., 2019. The Challenge of filling the Strategic Power Vacuum in the IndoPacific. Def. Secur. J. 4.

Kilcullen, D., 2010. Counterinsurgency. Oxford University Press.

Lehto, M., 2022. Cyber-Attacks Against Critical Infrastructure, in: Lehto, M., Neittaanmäki, P. (Eds.), Cyber Security: Critical Infrastructure Protection. Springer International Publishing, Cham, pp. 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Luddy, M.J., 2005. THE CHALLENGE AND PROMISE OF NETWORK-CENTRIC WARFARE.

Manangoda, M., 2022. The future of urban warfare: The development of training strategy. Def. Secur. J. 7, 45.

Mohee, A., 2022. A Realistic Analysis of the Stuxnet Cyber-attack. https://doi.org/10.33774/apsa-2022-qs797

Mumford, A., Carlucci, P., 2023. Hybrid warfare: The continuation of ambiguity by other means. Eur. J. Int. Secur. 8, 192–206. https://doi.org/10.1017/eis.2022.19

Muradov, I., 2022. The Russian hybrid warfare: the cases of Ukraine and Georgia. Def. Stud. 22, 168–191. https://doi.org/10.1080/14702436.2022.2030714

Naseeb, S., 2024. Hybrid Warfare: Blurring the Lines Between Conventional and

Non-Conventional Tactics. Int. J. Conv. Non-Conv. Warf. 1, 46–55.

Nye, J.S., 2018. Normative restraints on cyber conflict. Cyber Secur. Peer-Rev. J. 1, 331–342.

O'Neill, B.E., 1980. Insurgency: A Framework for Analysis, in: Insurgency In The Modern World. Routledge.

Otaiku, A.A., 2018. A Framework for Hybrid Warfare: Threats, Challenges and Solutions 8.

Pathirana, A.C., Nimesha, D., Palliyaguruge, S.S., Nazreen, Z., Nishadi, U., Nishamini, P., Ratnayake, H.E., Wickramasinghe, N.D., 2023. Burnout among Army personnel: A Sri Lankan Experience. https://doi.org/10.21203/rs.3.rs-3018462/v1

Pathirana, U., 2024. An Analysis of Social Integrating of Mass-Retiring Sri Lankan Armed Forces into Civil Context through the Security Lens. Sri Lanka Mil. Acad. J. 43–59.

Payne, S.F., 2017. Strategic choice: United States Special Forces' comparative advantage in irregular warfare.

Razma, G., 2019. A modern warfare paradigm: reconsideration of combat power concept /. J. Secur. Sustain. Issues 8, 435–452. https://doi.org/10.9770/jssi.2019.8.3(12)

Saunders-Price, B.B., 2020. Chapter 62 - Terrorism and warfare (chemical, biological, and radioactive and nuclear), in: Wexler, P. (Ed.), Information Resources in Toxicology (Fifth Edition). Academic Press, pp. 589–605. https://doi.org/10.1016/B978-0-12-813724-6.00062-1

Senaratne, B., 2017. Dynamics in Cybersecurity: Challenges to Sri Lanka`s National Security.

Shamieh, L., 2021. The Impact of Counterinsurgency on Human Security in Fragile States (PhD). Nemzeti Közszolgálati Egyetem, Budapest. https://doi.org/10.17625/NKE.2021.026

Sitaraman, G., 2009. Counterinsurgency, the War on Terror, and the Laws of War. Va. Law Rev. 95, 1745–1839.

Subramaniam, A., 2023. Pushing Boundaries: Can the Indian Military Transform? | EBSCOhost [WWW Document]. URL https://openurl.ebsco.com/contentitem/gcd:164670586?sid=ebsco:plink:crawler&id=ebsco:gcd:164670586 (accessed 4.30.25).

Taillat, S., 2024. Chapter 3: Conceptualizing cyberwarfare.

Tripodi, C., 2025. Fragmented frontiers: three approaches to understanding irregular warfare. Small Wars Insur. 0, 1–28. https://doi.org/10.1080/09592318.2025.2468941

US Department of Defence, 2007. Irregular Warfare (IW) Joint Operating Concept (JOC).

van Haaster, J., 2016. Assessing cyber power, in: 2016 8th International Conference on Cyber Conflict (CyCon). Presented at the 2016 8th International Conference on Cyber Conflict (CyCon), pp. 7–21. https://doi.org/10.1109/CYCON.2016.7529423

Velch, I., 2013. U.S. Army | Infantry Magazine [WWW Document]. URL https://www.benning.army.mil/infantry/magazine/issues/2013/May-June/Welch.html (accessed 4.30.25).

INTRODUCTION

1. This chapter provides a detailed and systematic discussion of the research approach and research design outlining the conceptual understandings with theoretical framework and process undertaken to examine the study's core argument and selected research questions. The study details the systematic approach for investigating the integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army to ensure the accuracy and credibility of the research. Hence, the chapter explains the methodological actions including the research approach, sampling and types of data, data collection methods and techniques of data analysis.

RESEARCH APPROACH

2. This study aims to adopts a qualitative research approach to explore the integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army. The focus will be on understanding the underlying challenges, existing practices and potential solutions through comprehensive qualitative methods having specific emphasis on identified case studies and to provide a comparative analysis with Australia and Pakistan doctrinal development.

3. This qualitative method enables the exploration of institutional, doctrinal and strategic levels of intervention for capability integration by extracting ideas and thaoughts from practitioners and experts with direct experience in hybrid warfare concepts. The study focuses on understanding perceptions, identifying patterns and extracting lessons learned rather than statistical generalization.

RESEARCH DESIGN

4. This study utilizes a qualitative design with an exploratory and descriptive approach to investigate into dynamic circumstances of the hybrid warfare capability

integration specifically in the Sri Lanka Army context. To gain an in-depth understanding of organizational, doctrinal, technological and financial challenges that could be viable with integrating conventional, irregular and cyber warfare capabilities, the primarily suitable approach is the qualitative approach.

5. The design enables the survey of individual experiences, perceptions and perspectives and insights from professionals both from military and academia. The design also employs a case study methodology focusing on the Sri Lanka Army as the prime concern of the analysis, while incorporating comparative essentials from other international military experiences specifically from Australia and Pakistan through their published doctrines and teachings related to hybrid warfare integration. This design allows for a comprehensive examination of the specific background, challenges and opportunities within the Sri Lankan defence backdrop while drawing valuable lessons from internationally updated practices.

THEORETICAL LENS

6. The foundational theoretical lens for the study is the 'Hybrid Warfare Theory' which emphasises the simultaneous and adaptive use of conventional, irregular and cyber means to fulfill strategic objectives (Sutil Toledano, 2023). This theory enables a comprehensive framework to understand the dynamic challenges of warfare integration. Additionally, considerations from 'Military Innovation Theory' guides the analysis of organisational learning and leadership aspects crucial for discussed integration (Modig and Andersson, 2022).

7. Boyd's OODA Loop (Observe, Orient, Decide and Act) theory or the decision action cycle also discusses to highlight the importance of speed, decentralisation and systematic thought process in adjusting with hybrid warfare scenarios. In combination, these theories provide the 'methodological and theoretical foundation' that necessitate for the research.

CONCEPTUAL FRAMEWORK

8. The study adopts a conceptual framework that visually and textually links the domains of conventional, irregular and cyber warfare. This emphasises the interdependencies of those aspects and the factors influence for their integration. This framework acts as a roadmap for the research, demonstrating how different warfare capabilities interact and shape each other. It directly highlights key integration challenges including organisational structures, technological limitations, financial constraints and existing doctrinal gaps while integrating proposed solutions derived from the research objectives and core argument also.

9. The theoretical foundation including the Hybrid Warfare Theory, offers a broad understanding of hybrid warfare and the necessity of integration (Gunneriusson, 2021). The conceptual framework then translates this theory into actionable insights by pinpointing specific components (conventional, irregular, cyber domains) with their interconnections and the difficulties (organizational, doctrinal, financial, technological) hindering integration within the Sri Lanka Army.

10. This close linkage ensures that the theories are not just discussed in Chapter Two but actively shape the research design and analysis. As a result, the study moves beyond descriptive findings to deliver a theoretically grounded analysis.

POPULATION AND SAMPLING

11. **Target Population.** The target population for this study includes Sri Lankan senior military officers, defence strategists and academic scholars who possess expertise in hybrid warfare, military integration and Sri Lankan defence and strategic studies. This population is based on their unique insights into the complexities of military operations, policy-making and strategic development.

12. **Sampling Method.** A purposive sampling method is employed to select key personnel who possess relevant expertise and experience in the subject matter. This non-probability sampling technique is appropriate for qualitative research as it allows the researcher to intentionally select information-rich cases that can provide deep insights into the research questions. The selection criteria prioritize individuals with

direct experience in strategic planning, command roles, or academic research related to the integration of warfare capabilities.

13. **Sample Size and Data Saturation.** The sample size is not predetermined by a fixed number but is guided by the principle of data saturation. Data saturation is reached when no new themes or insights emerge from additional data collection, and the researcher becomes empirically confident that a category or theme is fully developed. This ensures that sufficient depth and breadth of information are collected to address the research questions comprehensively without over-collecting redundant data. Relying on data saturation provides a robust, qualitative-specific justification for determining when to stop collecting data. This approach ensures that the research captures the necessary depth of information from the most relevant sources, thereby maximizing the quality and wealth of the data, even within potential access limitations. This demonstrates methodological flexibility and precision in a challenging research environment.

DATA COLLECTION METHODS

14. **Primary Data Collection.** Semi-structured interviews serve as the primary method for collecting qualitative data. This approach allows for a flexible yet guided conversation, enabling the researcher to explore pre-defined themes related to the research questions while also allowing for the emergence of new, unanticipated insights from the interviewees. Interviews gather expert insights on present procedures and integration challenges directly addressing research questions. A detailed interview protocol is developed, outlining key themes and open-ended questions designed to elicit rich, descriptive data. The protocol is aligned with the research objectives and core argument. Semi-structured interviews provide the necessary flexibility for the researcher to probe deeper into unexpected but relevant points raised by senior military officers and strategists. This adaptability is crucial for uncovering hidden challenges, unstated assumptions, or innovative solutions that might not be immediately apparent from existing literature or policy documents. It allows for a more comprehensive and nuanced understanding of the conceptual, moral and physical components of fighting power and their impact on integration.

Table 3.1: Interview Procedure and Key Themes

Ser	Research Objective	Key Theme	Sample Interview Questions
(a)	**(b)**	**(c)**	**(d)**
1.	To analyse the current state of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.	Current Capabilities & Gaps	What is your assessment of the current state of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army? What are the most significant strengths and weaknesses?
2.	To identify challenges in achieving integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.	Integration Challenges	What organizational, doctrinal, technological, or financial challenges hinder the effective integration of these capabilities? How do existing structures impact this integration?
3.	To evaluate strategies adopted by international militaries in hybrid warfare integration.	International Best Practices	What lessons can be drawn from international militaries' experiences in integrating warfare capabilities? Which foreign doctrines or strategies do you find most relevant or adaptable to the Sri Lankan context?
4.	To propose recommendations for the effective integration of conventional, irregular and cyber warfare capabilities within the Sri Lanka Army.	Proposed Reforms & Solutions	What specific reforms or initiatives are required to achieve effective integration of these capabilities within the Sri Lanka Army? What are the priorities for future development?

(a)	**(b)**	**(c)**	**(d)**
5.	How do organisational structures and doctrine support or hinder capability integration?	Organizational & Doctrinal Impact	Can you describe how the current organizational structures and military doctrine either facilitate or impede the integration of hybrid warfare capabilities?
6.	What specific reforms are required to achieve effective integration of these capabilities?	Reform Requirements	Beyond current plans, what concrete steps or policy changes are essential for successful integration, particularly concerning resource allocation and training?

Source: Developed by the researcher (2025)

15. **Secondary Data Collection.** A thorough review and analysis of secondary data sources complements the primary data. This includes policy documents initiated by Ministry of Defence of Sri Lanka, Sri Lanka Army doctrinal publications, journal articles published through Institute of National Security Studies, Centre for Law and Security Studies, Bandaranaike Center for International Studies and other military institutes of Sri Lanka related to hybrid warfare and military integration. Also, published papers on Australia and Pakistan hybrid warfare integration will be referred. Document analysis provides contextual background, historical perspectives, official policies and comparative insights from other nations' militaries. This is crucial for evaluating strategies adopted by international militaries and understanding the 'gaps of literature'. Documents are systematically identified, selected and reviewed based on their relevance to the research questions and objectives. A critical appraisal is conducted to assess the credibility and applicability of each document.

Table 3.2: Criteria for Secondary Data Selection

Ser	Criteria	Questions to Ask	Rationale for Inclusion
(a)	(b)	(c)	(d)
1.	Reliability	Who collected the data? What were the sources of data? Were they collected using proper methods? At what time were they collected? Was there any bias of the compiler? What level of accuracy was desired, and was it achieved?	Ensures the consistency and trustworthiness of the data, minimizing the risk of drawing conclusions from flawed or biased information.
2.	Suitability	Is the data's definition of terms, object, scope and nature aligned with the current inquiry? If differences are found, the data is unsuitable.	Confirms the relevance of the data to the specific research questions and objectives, preventing the use of information that does not directly contribute to the study's purpose.
3.	Adequacy	Is the level of accuracy sufficient for the purpose of the current inquiry? Is the area covered by the data appropriate (not too narrow or too wide) for the study?	Determines if the data provides sufficient depth and breadth to support robust analysis and conclusions, ensuring comprehensive coverage of the research problem.

Source: Developed by the researcher (2025)

DATA ANALYSIS METHODS

16. Thematic analysis serves as the primary method for analyzing the qualitative data collected from interviews and documents. This method is chosen for its flexibility and systematic approach to identifying, analyzing and reporting patterns (themes) within data. The process involves familiarization with the data, initial coding, searching for themes, reviewing themes, defining and naming themes and producing the report.

17. The analysis aims to describe and summarise the data and turn raw numbers into meaningful data through application of rational and critical thinking. The analysis is

expressed primarily in words, reflecting the thematic analysis of the data and guiding the reader through the evolved themes.

ETHICAL CONSIDERATIONS

18. **Ethical Clearence.** Formal ethical clearance is obtained from the Defence Services Command and Staff College (DSCSC) and the General Sir John Kotelawala Defence University (KDU) prior to the commencement of any data collection, as per institutional guidelines. Also, the study obeyed to ethical guidelines and principles throughout the process by ensuring the participants' willingness, rights, dignity and comfort. Prior to interviews, participants are provided with clear information about the study's purpose, procedures, their right to withdraw at any time and how their data will be used. Their voluntary informed consent is obtained, typically in writing, before the interview commences.

19. **Confidentiality and Anonymity.** Participants are assured that their identifying information will be kept strictly confidential and will not be made available to anyone not directly involved in the study or published in the research report. Anonymity is maintained in all reporting and dissemination of findings, using pseudonyms or aggregated data where appropriate. The emphasis on ethical clearance and confidentiality is particularly critical in military research due to the sensitive nature of information and the hierarchical structure of the organization. Hence, ensuring confidentiality is paramount to encourage participants to share honest insights without fear of professional repercussions. Without strong assurances of confidentiality, the quality and depth of qualitative data could be severely compromised. The research design and data collection procedures are structured to minimize any potential physical or psychological harm to participants. Questions are framed sensitively and interviewer (researcher) is trained to handle potentially delicate topics with care. All collected data including interview transcripts and recordings are stored securely on password-protected devices and accessible only to the researcher, ensuring compliance with data protection principles.

INTRODUCTION

1. This chapter presents the findings of the study. It answers the research questions and addresses the objectives. The focus is the integration of conventional, irregular and cyber warfare capabilities in the Sri Lanka Army. Hence, the analysis uses evidence from interviews and documents. The researcher uses a qualitative design. It adopts an exploratory and descriptive approach. The Sri Lanka Army is the main case.

2. Primary data come from semi-structured interviews. Participants include senior military officers, defence strategists and scholars. Purposive sampling has guided the selection. Data saturation determined the final sample. An interview protocol aligned with the objectives and key themes. The questionnaire guided the interviews.

3. Secondary data include policy and doctrinal publications. They also include journal articles and relevant reports. Comparative documents from foreign militaries are also used when needed. Selection followed clear criteria for reliability, suitability and adequacy. The study applies a thematic analysis. Coding and theme development follow standard steps. Themes link back to the objectives and research questions.

4. Ethical standards have guided all procedures. Approvals were obtained before data collection. All identities of interviewees have kept confidential. Quotes are anonymised and paraphrased for the presentation. Data are stored securely.

5. Basically, the chapter is organised around four themes. First, current capabilities and gaps. Second, integration challenges. Third, international best practices. Fourth, proposed reforms and future directions and further mentioned under table 4.1. These themes mirror the interview guide and the objectives.

THEMATIC ANALYSIS AND CODING

6. The qualitative data collected from interviews were examined using thematic analysis. This process involved several steps. First, the interview transcripts were read

multiple times to gain familiarity. Second, initial codes were created by marking recurring words, phrases and ideas related to the research questions. Third, these codes were grouped into broader categories. Finally, the categories were refined into key themes that align with the objectives of the study.

7. The coding process was both inductive and deductive. Some codes were drawn directly from participant language, such as "outdated equipment" or "lack of cyber skills." Others were guided by the research objectives, for example "integration challenges" or "international best practices." This combination ensured that the analysis remained rooted in participant voices while also addressing the academic aims of the study. The table 4.1 presents the coding framework used in this study:

Table 4.1: Coding Framework of the Study.

Ser	Research Objective	Codes	Themes
(a)	(b)	(c)	(d)
1.	Analyse current capabilities	a. Outdated equipment b. Strong combat experience, c. Irregular warfare skills d. Weak cyber defence	Current capabilities and gaps
2.	Identify integration challenges	a. Rigid hierarchy b. Outdated doctrine c. Limited budget d. Lack of cyber skills	Challenges to integration
3.	Evaluate international practices	a. US cyber command b. Indian IBGs c. Pakistan COIN-cyber d. Australian doctrine focus	Lessons from international best practices
4.	Propose reforms and priorities	a. Establish cyber command b. Hybrid doctrine c. Tri-service integration d. Affordable tech adoption	Proposed reforms and future directions

Source: Developed by the author (2025)

8. The analysis revealed four broad themes. Each theme is supported by several codes drawn from the interviews. For example, codes such as *"outdated equipment"*, *"dependence on manpower"* and *"weak cyber defence"* were grouped together under the theme of **Current capabilities and gaps**. Similarly, codes including *"rigid*

hierarchy" and *"doctrine outdated"* were placed under the theme of **Challenges to integration**.

9. The distribution of codes across the four themes is illustrated in the figure 4.1 below. Each theme was supported by multiple codes, showing that participants consistently provided insights in all areas of inquiry.

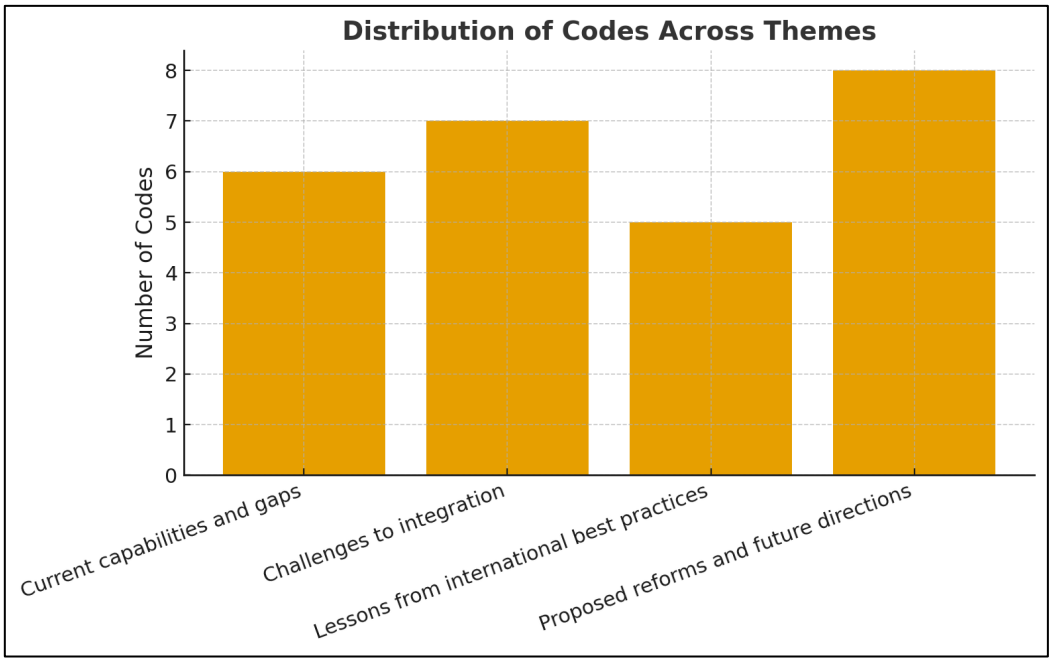

Figure 4.1: Distribution of Codes Across Themes.
Source: Developed by the author (2025)

10. The coding process showed that the number of codes varied across themes. The chart above illustrates this distribution. The highest number of codes appeared under Proposed reforms and future directions. This indicates that many participants were eager to suggest changes, highlighting the importance of reform in their perspectives.

11. The second largest set of codes fell under Challenges to integration. This reflects the wide range of barriers raised by respondents, including structural, doctrinal, financial and cultural issues. It suggests that participants were strongly aware of obstacles that currently prevent the Army from achieving effective integration.

12. A moderate number of codes were grouped under Current capabilities and gaps. This demonstrates that while participants recognised both strengths and weaknesses in

conventional, irregular and cyber domains, they placed more emphasis on the need for change than on the existing situation.

13. The smallest number of codes were associated with Lessons from international best practices. Although participants referred to models such as the United States, Russia, India, Pakistan, and Australia, they generally kept these references brief. Their focus was less on foreign cases and more on how Sri Lanka should adapt its own approach.

14. This pattern shows that participants were forward-looking and solution-oriented. They acknowledged challenges and gaps but invested more energy in recommending reforms. This distribution reinforces the argument that the Sri Lanka Army is at a turning point where the demand for transformation is both recognised and urgent.

CURRENT CAPABILITIES AND GAPS OF THE SRI LANKA ARMY

CONVENTIONAL WARFARE

15. The Sri Lanka Army's strength in conventional warfare is well established. Decades of conflict have built a large pool of officers and soldiers with combat experience. Senior officers interviewed often described this as a "battle-hardened force." One retired General stated, "Our Army has been tested in real wars, not just exercises. That experience is a strength that cannot be replaced by any technology alone."

16. The Army has demonstrated the ability to conduct joint operations with artillery, armour and infantry. Interviewees recalled that during the final years of the conflict, small independent teams were effectively supported by heavy weapons and air assets. This was highlighted as evidence that the Army knows how to coordinate across branches.

17. Yet, several limitations were raised. Participants pointed out that much of the Army's equipment is outdated. Tanks, artillery and armoured vehicles require upgrades. A Director from AHQ commented, "We have manpower and morale, but our platforms are too old. We are fighting with yesterday's tools." Another respondent stressed the lack of precision strike capability, saying, "We still depend on volume of firepower. Modern armies focus on accuracy, not just numbers."

18. Thus, while conventional skills remain strong, the technological base has not kept pace. The Army can fight conventionally but risks being overmatched if confronted by a technologically advanced adversary

IRREGULAR WARFARE

19. Irregular warfare emerged as another area of relative strength. Many officers reflected on the lessons learned from the LTTE conflict. A retired commander remarked, *"The Tigers forced us to adapt every day. We learned to fight like them — small units, raids, deception. That knowledge is in our blood."*

20. Interviewees described irregular capabilities such as jungle operations, counterinsurgency, and deep penetration tactics as unique assets of the Army. They also recalled the innovative methods developed during the war, including naval-style littoral operations and early use of information warfare.

21. However, concerns were raised about whether these skills are being preserved. A commandant of a training institute explained, *"Our training now is more focused on drills and conventional tasks. We don't get the same exposure to irregular operations."* Another strategist observed that irregular threats are evolving: *"Today's challenges are not LTTE-style. They are extremist cells, organised crime, and even cyber-enabled insurgency. We are not fully ready for those."*

22. This suggests that while irregular warfare experience is rich, institutional memory is at risk of fading. Without structured programmes to retain and adapt this knowledge, the Army could lose one of its main advantages

CYBER WARFARE

23. The cyber domain was consistently described as the weakest area. Respondents agreed that Sri Lanka lacks both infrastructure and skilled personnel. One senior officer involved in IT noted, *"We have a Cyber Security Cell, but it is small and focused only on defence. Offensive capacity is almost non-existent."* Another officer added, *"We depend on commercial systems. Even our networks are not fully secure."*

24. Some progress has been made, particularly in partnerships with SLCERT and the introduction of AI-based monitoring tools. However, these steps are modest. Participants stressed the absence of a dedicated **Cyber Command**. A defence academic summarised, *"Every modern army recognises cyber as a fifth domain. We are still treating it as an add-on."*

25. The gap is not only technical but also cultural. Several interviewees admitted that many officers view cyber as "support" rather than a core combat function. This mindset limits investment and slows development.

OVERALL GAPS

26. When asked to compare all three domains, participants described an imbalance. Conventional warfare remains the backbone, irregular warfare is respected but fading, and cyber is underdeveloped. One strategist summarised, "We are a two-legged soldier trying to run a three-legged race. Until cyber develops and all three legs are balanced, integration will remain theory."

27. The overall finding is that the Sri Lanka Army has strong conventional and irregular roots but lacks cyber maturity. More importantly, the three domains have not yet been integrated. Planning and training continue to treat them as separate entities. This prevents the creation of hybrid synergy, where the combined effect of conventional, irregular, and cyber would be greater than their individual strengths.

CHALLENGES TO INTEGRATION

ORGANISATIONAL AND STRUCTURAL CHALLENGES

28. Several officers described rigid structures as the main barrier. One director noted, *"Our organisation is too vertical. There is little cross-talk between branches."* Another emphasised the lack of jointness with Navy and Air Force. *"We do joint exercises, but hybrid integration is not institutionalised,"* he said.

DOCTRINAL CHALLENGES

29. Doctrinal gaps also stood out. A strategist explained, *"The Capstone Doctrine is too general. It does not tell us how to merge cyber with irregular and conventional."* Others described planning as still conventional-heavy. As one strategist put it, *"Doctrine has not yet caught up with modern threats."*

TECHNOLOGICAL CHALLENGES

30. Technology was seen as both essential and limited. An IT expertise remarked, *"We do not own advanced surveillance or cyber tools. We depend on foreign systems."* Another respondent highlighted weak research and development in Sri Lanka. The lack of secure networks was mentioned by several participants as a serious concern.

FINANCIAL CHALLENGES

31. Budget constraints were repeatedly mentioned. A senior officer explained, *"Eighty percent of the budget goes to salaries. That leaves little for new equipment."* A defence scholar added, *"Modernisation requires investment, but financial realities keep us behind."*

CULTURAL AND MINDSET CHALLENGES

32. Many respondents spoke of a cultural lag. *"Our officers still think in terms of tanks and artillery,"* one participant noted. Another added, *"There is hesitation to embrace cyber or hybrid thinking. Some view it as theoretical rather than practical."* Several stressed that without a change in mindset, reforms will struggle.

LESSONS FROM INTERNATIONAL BEST PRACTICES

UNITED STATES

33. Several interviewees highlighted the US model as the most advanced in integrating conventional, irregular and cyber warfare. A defence scholar explained, *"The JADC2 system is a good example of how technology links every domain. It connects land, air, sea, cyber and space in real time."* Participants admired the institutionalisation of USCYBERCOM, which operates alongside conventional and special forces.

34. However, officers also expressed caution. One strategist noted, *"We cannot copy the American model. It is expensive and requires a huge technological base. But we can learn the principle of jointness and shared networks."* This suggests that while the US approach offers inspiration, Sri Lanka must adapt lessons to its scale and resources.

RUSSIA

35. Participants often referred to Russia's hybrid operations in Ukraine and Georgia. A senior officer remarked, *"Russia shows how cyber, disinformation and militias can support conventional forces."* Another added, *"They create confusion, so the enemy cannot tell what is war and what is peace."*

36. Yet some respondents warned against over-reliance on the Russian example. One academic observed, *"Russia's approach is aggressive and politically costly. For Sri Lanka, the lesson is not to copy but to understand the value of ambiguity and information control."* This indicates a selective adoption of insights, focusing on strategic messaging and psychological operations rather than outright imitation.

INDIA

37. India's model was viewed as highly relevant for Sri Lanka. A civiliasn scholar commented, *"India has similar regional challenges. Their Defence Cyber Agency is small but functional. That is something we can aim for."* Another participant praised the Integrated Battle Groups, saying, *"They show how to be flexible with limited resources."*

38. Several interviewees stressed the cultural proximity. *"We can cooperate with India in training and cyber defence. Our militaries understand each other better than with the West,"* one officer explained. This reflects a practical route for Sri Lanka, where regional partnerships and scalable reforms are more realistic than adopting distant models.

PAKISTAN

39. Pakistan was cited as an example of how a country under financial constraints still manages hybrid threats. A defence strategist explained, *"Pakistan has focused on counterinsurgency and cyber at the same time. They built capacity gradually, not overnight."*

40. A general who had studied in Pakistan noted, *"They blend irregular and conventional training. Even at tactical level, soldiers are exposed to hybrid thinking."* This suggests a valuable lesson for Sri Lanka: hybrid warfare must be taught from the lowest levels, not only at staff colleges.

AUSTRALIA

41. Australia's emphasis on doctrine and training was seen as instructive. A respondent highlighted, *"Australia builds everything around doctrine. That way, even new domains like cyber are integrated into education."* Another participant remarked, *"They may not face daily wars like us, but their preparation is systematic. We need that mindset."*

42. The lesson from Australia, according to many, is not technology but organisation. Clear doctrine and structured training help smaller militaries adapt faster. As one officer summarised, *"We cannot buy advanced tools quickly, but we can build doctrine and train with what we have."*

CROSS-CUTTING LESSONS

43. Across the interviews, certain common lessons emerged:

a. **Institutionalisation is Key.** Countries succeed when integration is anchored in formal structures like commands or agencies.

b. **Doctrine Drives Changes.** Where doctrine emphasises hybrid threats, training and operations follow naturally.

c. **Technology must be Adapted to Scale.** Large powers invest in expensive systems. Smaller states adopt selective, cost-effective measures.

d. **Regional Cooperation Matters.** Lessons from neighbouring countries often apply better than distant models.

44. One strategist summarised, *"The lesson from abroad is not to imitate but to adapt. Hybrid integration is not one formula. Each country does it differently. We must design a Sri Lankan way."*

PROPOSED REFORMS AND FUTURE DIRECTIONS

ORGANISATIONAL REFORMS

45. Many participants emphasised the need for new structures within the Army. Several officers suggested a **dedicated Cyber Command**. One retired general stated, *"Without a cyber command, we are fighting with one arm tied. A small unit under IT cannot handle future wars."* Another strategist added, *"Integration requires hybrid units where conventional, irregular and cyber elements work together."*

46. Others called for stronger **jointness with Navy and Air Force**. A senior officer noted, *"We cannot face hybrid threats as Army alone. Tri-service integration must go beyond exercises and become permanent."* This suggests that organisational reform is central, including creation of hybrid task forces and joint planning cells.

DOCTRINAL REFORMS

47. Respondents strongly argued for doctrinal changes. The "Capstone Doctrine" was seen as useful but incomplete. An academic remarked, *"Doctrine should tell us how cyber supports ground troops, or how irregular units fit into joint operations. Right now, it does not."* Another officer proposed a **Hybrid Warfare Doctrine** as a supplement to the Capstone.

48. Several interviewees also stressed doctrinal revision in training. *"Doctrine is not just a book. It shapes what we teach in our academies. If hybrid is not in doctrine, it is not in training,"* one officer explained. This highlights the importance of doctrine as a driver of cultural change.

TECHNOLOGICAL REFORMS

49. Participants repeatedly called for investment in technology. One IT expertise noted, *"We need secure networks, not just commercial systems. Our current infrastructure is too vulnerable."* Others pushed for gradual adoption of **AI-based tools, drones and surveillance systems**.

50. A defence strategist emphasised, *"We do not need the most expensive systems. Even low-cost but smart technology can give us hybrid advantage."* The consensus was that technology should be scaled to Sri Lanka's budget, but it must still form the backbone of integration.

TRAINING AND EDUCATION

51. Training was a dominant theme across the interviews. A commandant of a training institute commented, *"We need hybrid concepts taught from cadet school. Not only at staff college."* Another explained, *"Our soldiers must be comfortable in both conventional and irregular settings. Cyber awareness should be basic training for all."*

52. Respondents recommended updating the curriculum at the **Sri Lanka Military Academy, Army Training Centre, Army War College, Defence Services Command and Staff College and National Defence College**. They also called for joint exercises with Navy and Air Force focused on hybrid scenarios. One academia added, *"Simulations and war-gaming in hybrid context are low-cost but high value. We are not using them enough."*

REGIONAL AND INTERNATIONAL PARTNERSHIPS

53. Several officers viewed partnerships as critical. An interviewee stated, *"We must work with India for cyber training. They are close and understand our*

environment." Others mentioned cooperation with the US and Australia for technical expertise. A strategist explained, *"Partnerships should be practical. Not only workshops, but joint projects, secondments and shared platforms."*

54. At the same time, some warned of dependency. *"Partnerships should not make us over-reliant. We must use them to build our own capacity,"* one officer cautioned. This suggests a careful balance between learning from others and maintaining independence.

PRIORITY AREAS FOR THE NEXT 5–10 YEARS

55. When asked about priorities, participants provided clear and consistent responses.

a. **Establish a Cyber Command.** Most participant saw the establishment of Cyber Command as an urgent demand.

b. **Develop a Hybrid Warfare Doctrine.** This would shape future training and operations.

c. **Strengthen Tri-service Integration.** Hybrid threats demand permanent jointness.

d. **Invest in Selective Technology.** Affordable cyber tools, drones and secure networks.

e. **Revise Training.** Hybrid concepts introduced from the lowest levels.

THEMATIC CROSS-ANALYSIS

56. The findings from interviews and secondary data reveal several recurring themes. These themes reflect both strengths and weaknesses in the Sri Lanka Army's path towards integration of conventional, irregular and cyber warfare.

57. **The Balance between Domains.** Interviews confirmed that the Army remains strongest in conventional and irregular operations, shaped by decades of conflict with the LTTE. Literature also highlighted Sri Lanka's mastery of counterinsurgency tactics. However, both sources agree that cyber remains underdeveloped. While Western and regional militaries have institutionalised cyber commands, Sri Lanka is still at an early stage.

58. **Organisational Rigidity.** Participants described a vertical command structure with limited cross-talk. This aligns with studies pointing out that hybrid warfare requires flatter, networked systems. The absence of jointness with Navy and Air Force was a common concern. Comparative cases, such as US JADC2 or India's Integrated Battle Groups, show how integration is accelerated by structural reform.

59. **Doctrinal Pause.** Both interviews and literature emphasised that doctrine does not fully reflect hybrid realities. While the Capstone Doctrine provides a broad base, it lacks specific guidance on merging cyber, irregular and conventional elements. These finding echoes international research stressing the central role of doctrine in driving adaptation.

60. **Financial and Technological Barriers.** Interviewees repeatedly mentioned funding constraints. Most of the budget is spent on salaries, leaving little for modernisation. Literature also noted this challenge. At the same time, interviewees suggested that selective, low-cost technology could still deliver hybrid benefits, which is consistent with smaller state practices worldwide.

61. **Cultural Resistance.** Interviews revealed that many officers remain rooted in conventional thinking. Literature on military innovation theory describes similar challenges in other armed forces, where cultural adaptation often lags behind structural reform. The Sri Lanka Army is not unique in this, but it shows the need for deliberate mindset change.

62. **Lessons from Foreign Armies.** Participants pointed to the US, Russia, India, Pakistan and Australia as models. Their reflections confirm the literature: large powers show the importance of institutionalisation and technology, while regional examples demonstrate practical and affordable pathways. The consensus was that Sri Lanka should adapt rather than copy.

63. Across interviews, five consistent priorities emerged as follows:

a. A cyber command.

b. A hybrid warfare doctrine.

c. Stronger jointness with sister services.

d. Selective technology.

e. Revised training modules

64. These themes closely match the gaps identified in Chapter Two and the research questions outlined in Chapter One.

CONCLUSION

65. This chapter drew on qualitative interviews with senior officers, defence strategists and scholars, supported by secondary sources. The analysis followed four main themes as current capabilities and gaps, integration challenges, lessons from international best practices and proposed reforms.

66. The findings show that the Sri Lanka Army has strong conventional and irregular capacity but limited cyber strength. Integration across domains is weak.

Organisational structures, doctrinal gaps, financial constraints, technological limits and cultural resistance all hinder progress. At the same time, there is awareness within the Army of the need for change.

67. International models offer useful lessons. Larger powers highlight the value of institutionalised cyber commands and joint networks. Regional neighbours show how smaller militaries can adapt within constraints. Interviewees stressed that Sri Lanka must build its own approach rather than copy others.

68. The chapter concludes that integration is both necessary and possible. The Army requires structural reform, doctrinal innovation, selective technology and training for hybrid readiness. The establishment of a cyber command and a dedicated hybrid warfare doctrine emerged as the most urgent reforms. These findings provide the foundation for Chapter Five. The next chapter will discuss their implications, connect them with theory and explore how the Sri Lanka Army can move from findings to implementation.